CLAIMS

1. A method for detecting malicious applications in an electronic messaging environment, comprising:

implementing a security software application in an electronic messaging system with connection to a data network;

providing a local configuration of the security software application on a local messaging terminal, wherein the local configuration includes a list of at least one known malicious application;

detecting an electronic message received or to be sent by a local messaging terminal;

determining whether the electronic message includes any attachment;

if an attachment is included with the electronic message, using the security software application to check the attachment for any malicious application based on the list of at least one known malicious application;

refreshing the local configuration of the security software application from a globally replicated public folder within the electronic messaging system on a desired periodic basis.

2. The method of claim 1, wherein implementing a security software application on a local messaging terminal includes implementing an add-in software component to an electronic message client software of the electronic messaging system.

3. The method of claim 2, wherein the electronic message client software resides in a host server for the local messaging terminal.

4. The method of claim 1, wherein the security software application includes a dynamic link library (DLL) application.

5. The method of claim 1, further comprising:

prompting an error message on the local messaging terminal when the attachment to the electronic message matches a name on the list of the at least one known malicious application.

6. The method of claim 5, further comprising:

blocking the matched attachment from being opened or sent.

7. The method of claim 1, wherein the list of at least one known malicious application includes a list of known virus filenames.

8. The method of claim 1, wherein the local configuration of the security software application includes:

an option to enable a checking of an attachment for any malicious application based on the list of at least one known malicious application;

an option to add or remove a known malicious application from the list of at least one known malicious application; and

an option to restrict an attachment type.

9. The method of claim 1, wherein the local configuration of the security software application includes an option to set a time for the desired periodic basis to refresh the local configuration.

10. A method for detecting malicious applications in an electronic messaging environment, comprising:

implementing a security software application in an electronic messaging system with connection to a data network;

providing a local configuration of the security software application on a local messaging terminal, wherein the local configuration includes a list of at least one application type;

detecting a receipt of an electronic message sent to a local messaging terminal;

determining whether the electronic message includes any attachment;

if an attachment is included with the electronic message, using the security software application to check the attachment for any malicious application based on the list of at least application type;

refreshing the local configuration of the security software application from a globally replicated public folder within the electronic messaging system on a desired periodic basis.

11. The method of claim 10, wherein implementing a security software application on a local messaging terminal includes implementing an add-in software component to an electronic message client software of the electronic messaging system.

12. The method of claim 11, wherein the electronic message client software resides in a host server for the local messaging terminal.

13. The method of claim 10, wherein the local configuration of the security software application includes:

an option to enable a checking of an attachment for any malicious application based on a list of at least one known malicious application;

an option to enable a checking of an attachment for a restricted application type based on the list of at least one application type; and

an option to add or remove an application type from the list of at least one application type.

14. The method of claim 10, wherein the list of at least one application type comprises executable application types.

15. The method of claim 14, wherein using the security software application to check the attachment comprises:

determining whether the attachment is of one of the executable application types listed in the list of at least one application type; and

if the attachment is of one of the executable application types, blocking the attachment from being opened or sent through the electronic messaging system.

16. The method of claim 10, wherein the list of at least one application type comprises application types not capable of containing malicious applications.

17. The method of claim 16, wherein using the security software application to check the attachment comprises:

determining whether the attachment is of one of the application types not capable of containing malicious applications; and

if the attachment is of one of the application types not capable of containing malicious applications, allowing the attachment to be opened or sent through the electronic messaging system.

18. The method of claim 10, wherein the local configuration of the security software application includes an option to set a time for the desired periodic basis to refresh the local configuration.